UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,561	08/16/2001	Marinus Frans Kaashoek	12221-003001	4263

26161 7590 05/09/2005

FISH & RICHARDSON PC
225 FRANKLIN ST
BOSTON, MA 02110

EXAMINER	
WRIGHT, NORMAN M	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 05/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,561	KAASHOEK ET AL.	
	Examiner	Art Unit	
	Norman M. Wright	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/23/05*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

5/4/05

NORMAN M. WRIGHT
PRIMARY EXAMINER
Art 2134

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12/23/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. *Claims 1-36 are present for examination.*

Claim Objections

2. Claims 2-3, 5, and 7-8, are objected to because of the following informalities: the use of 'hardened" is inconsistent with claim 1. Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fletcher et al., U.S. Pat. No. 6,108,782, hereinafter '782, in view of Cox U.S. Pat. No. 6,738,814, hereinafter '814.

As per claims 1, 12, 15 and 28, '782 teaches the invention of a method and system for remote monitoring in a distributed environment comprising: a data center, any element that may come under attack, coupled to a network (Lans, Wans etc.), monitoring traffic/ plurality of monitors (Rmon/probes/ monitors/ dRmons), disposed at a plurality of points (network devices, Is, hubs, switches, bridges, may also be any network device), communicating data from the monitors to a redundant network, and a central controller/dRmon collector (RMON-independent probe/monitor), collecting statistical data, performing analysis, and filtering (col. 4, lines 5-55, col. 6, lines 25-65 et

seq., col. 7, lines 35 et seq., figs. 1 and 8), DRMON manager, (fig. 1, col. 4, lines 5 – 54 et seq., col.5, lines 1-10 et seq., and 50 –64 et seq., col. 6, lines 10 et seq., col. 7, lines 47 et seq., col. 8, lines 20-29 et seq., lines 45-55 et seq.), plural monitors and plural points/groups or domains (fig. 8, col. 6, lines 47 et seq., col. 7, lines 34-41 et seq., and col. 18, lines 51 et seq.) and collection across different networks (cols. 7, lines 35 et seq., and col. 8, lines 20-55 et seq., col. 9, lines 33 et seq., col. 10, lines 34 et seq., col. 20, lines 16 et seq.). Not explicitly taught is the rule set for the filtering and/or collection mechanisms being that to detect a denial of service attack.

Cox teaches a method for blocking denial of service attack, comprising: a private (12) and public network (14), having a victim data center/point or object of attack (col. 1, lines 23 et seq.), and monitoring means to intelligently analyze the incoming packets (col. 1, lines 60-65 and col. 3, lines 25 et seq.). It would have been obvious to one of ordinary skill in the art at the time of the invention, to augment the invention of '782 with the programming means of '814 as a filtering or probe monitoring program. One of ordinary skill in the art would have been able to perform this modification by having a program, subroutine, or firmware installed in the dRmon's software of hardware monitoring/collecting modules. A person of ordinary skill in the art would have been motivated to perform such a modification because, '814 recites that there is an increasing pattern of denial attacks being performed at network routing devices (col. 1, lines 24-37). '782 teaches that it is desirable to have Rmons implemented as independent distributed network probes, because of the advantages it offers in performance monitoring and enhanced remote monitoring (col. 4, lines 5-55 et seq., col.

20, lines 43 et seq.). A person of ordinary skill would have readily envisaged that the use of distributed Rmons, via programming of their filtering routines, could readily be programmed to detect potentially harmful packed, such as a denial of service attack. So that, by having distributed Rmons within a network systems that the potential for detecting malicious attacks would be greatly increase, and security of the system enhanced.

As per claims 2-3, '782 teaches that the Rmons may be placed in an promiscuous mode/inaccessible, whereby both '782 and 814 teach that the monitoring needs to occur at gateways, hubs, bridges, switches, firewalls or any potential routing device (respectively, col.4, lines 1-20, 45-55, col. 8, lines 37 et seq.; and col. 1, lines 23-37).

As per claims 4-6 and 8 the incorporation of the filtering program into '782 would perform the same function of discarding malicious traffic at '814, col. 3, lines 67 et seq., denitrifying malicious traffic and entry points (col. 4, lines 1-15).

As per claims 7 and 9-11, '782 teach that Rmon probes may be placed at any point of desired monitoring and that the network devices and controllers may function as redundant element to other probes and monitors to avoid a failure leaving the system vulnerable (col. 4, lines 40-55, col. 5, lines 38-48, col. 6, col. 7, lines 35 et seq., col. 8, lines 40 et seq., col. 9, lines 33 et seq., and col. 10, lines 34 et seq.).

As to claims 23-24, as understood peering points are where different systems/networks meet. The collectors of '782 collect data across different networks and are positioned at peering points (figs. 1, col. 6, lines 25 et seq., col. 8, lines 37 et

seq., col. 9, lines 33 et seq.), and similarly see '814 at (col. 1, lines 23 et seq., col. 2, lines 45 et seq., col. 3, lines 23 et seq.).

As per claims 13-14, 16-22, 25-26, 29-35, recites the concomitant elements of rejected claims 1-12, 15, and 28, accordingly see above for the specifics of the rejections.

As to claims 27 and 36, '782 as modified by '814 would perform the function of having administrators heuristically monitor the trafficking of packets (see '814 at col. 3, lines 20 et seq., col. 4, lines 41 et seq.).

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

4. Claim1, 4, 6, 8, 12, 15, and 28 are provisionally rejected under the judicially created doctrine of double patenting over claims 1, 8, 15, 17, 20, 22, and 24 of copending Application No. 10/062,974. This is a provisional double patenting rejection since the conflicting claims have not yet been patented.

The subject matter claimed in the instant application is fully disclosed in the referenced copending application and would be covered by any patent granted on that copending application since the referenced copending application and the instant application are claiming common subject matter, as follows: a monitoring device/gateway, a plurality of probes/data collectors of gateway, collecting statistical information, a data center, networks, joining, victim data center, controller/cluster head (collectively 27, 33), interface (30), install filters, determining a denial of service attack, communication, identifying malicious traffic, analyzing and eliminating.

Furthermore, there is no apparent reason why applicant would be prevented from presenting claims corresponding to those of the instant application in the other copending application. See *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968). See also MPEP § 804.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Norman M. Wright whose telephone number is (703) 305-9586. The examiner can normally be reached on 5/4/9 compressed week.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

5/4/05.

Norman M. Wright
Primary Examiner
Art Unit 2134

nmw